KEBIJAKAN KRIMINAL PEMERINTAH TERHADAP KEJAHATAN DUNIA MAYA (*CYBER CRIME*) DI INDONESIA

Oleh: Endang Prastini
Dosen FKIP Universitas Pamulang
Jl. Surya Kencana Satu Pamulang Tangerang Selatan
Email: eprastini81@yahoo.com

Abstrak

Kebijakan kriminal merupakan suatu bentuk kebijakan yang diambil oleh suatu negara untuk melakukan kriminalisasi terhadap suatu tindakan yang dianggap merugikan, serta strategi untuk meanggulanginya. Dengan merujuk pada 3 (tiga) peran utama dari kebijakan, yaitu pembuatan kebijakan, pelaksanaan kebijakan, dan advokasi kebijakan. Pada hakikatnya kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*Criminal Policy*) dengan menggunakan sarana hukum pidana (penal), dan oleh karena itu merupakan bagian dari "Kebijakan Hukum Pidana (*penal policy*) khususnya kebijakan formulasinya. Penegakan hukum *Cyber Crime*di Indonesia sangat dipengaruhi oleh 5 (lima) faktor, yaitu undang-undang, mentalitas aparat penegak hukum, perilaku masyarakat, sarana dan kultur. Hukum tidak bisa tegak dengan sendirinya karena selalu melibatkan manusia dan tingkah laku manusia di dalamnya. Selain itu, hukum juga tidak bisa tegak tanpa adanya aparat penegak hukum. Oleh sebab itu, aparat penegak hukum dituntut profesional dalam menerapkan norma hukum dalam menghadapi pelaku tindak kejahatan. Kitab Undang-Undang Hukum Pidana (KUHP) menjadi dasar untuk menjaring *Cyber Crime,* yang memenuhi unsur-unsur dalam pasal-pasal KUHP.Selain KUHP ada juga aturan hukum yang berkaitan dengan hal ini, yaitu Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), dimana aturan tindak pidana yang terjadi di dalamnya terbukti mengancam para pengguna internet.
Key Word: Kebijakan Kriminal, Kejahatan Dunia Maya (*Cyber Crime*)

Abstract

Criminal policy is a form of policy taken by a country to criminalize an action that is considered detrimental, as well as a strategy to respond to it. By referring to 3 (three) main roles of policy, namely policy making, policy implementation, and policy advocacy. In essence the criminalization policy is part of the Criminal Policy by using criminal law (reasoning), and because it is part of the "Criminal Law Policy", especially the formulation policy. The law enforcement of Cyber Crimedi Indonesia is strongly influenced by 5 (five) factors, namely the law, the mentality of law enforcement officials, the behavior of the community, facilities and culture. The law cannot stand by itself because it always involves humans and human behavior in it. In addition, the law also cannot be upheld without the existence of law enforcement officers. Therefore, law enforcement officials are required to be professional in applying legal norms in dealing with criminals. The Criminal Code (KUHP) is the basis for capturing Cyber Crime, which fulfills the elements in the articles of the Criminal Code. In addition to the

Criminal Code there are also legal rules relating to this matter, namely the Law of the Republic of Indonesia Number 19 Year 2016 concerning Amendment to Law Number 11 Year 2008 concerning Information and Electronic Transactions (ITE), where the rules of criminal acts that occur in them are proven to threaten internet users.
Key Word: Criminal Policy, Cybercrime (Cyber Crime).

A. Pendahuluan

Pembangunan Nasional di Indonesia telah mencapai era tinggal landas, hal ini ditandai dengan meningkatnya era globalisasi yaitu adanya pertumbuhan ekonomi dan perkembangan pemanfaatan Ilmu Pengetahuan (IPTEK). Dalam hal ini produk IPTEK tersebut yang berkembang adalah teknologi komputer yang hampir menguasai seluruh aspek masyarakat modern.[1] Perkembangan teknologi dewasa ini semakin pesat. Khususnya teknologi telekomunikasi dan teknologi komputer yang menghasilkan internet dengan berbagai multifungsi, menggiring kita berfikir ke arah yang tanpa batas (*bordelles way of thinking*).[2]

Era globalisasi telah menempatkan peranan teknologi informasi ke dalam suatu posisi yang sangat strategis karena dapat menghadirkan suatu dunia tanpa batas, jarak, ruang, dan waktu serta dapat meningkatkan produktivitas serta efisiensi. Teknologi informasi telah merubah pola hidup masyarakat secara global dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangung secara cepat dengan signifikan.[3] Teknologi Informasi bagaikan pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.[4]

Penggunaan teknologi internet banyak menyelesaikan persoalan yang rumit secara efektif dan efisien. Selain itu, kecanggihan teknologi membuat orang cenderung melakukan perbuatan yang bertentangan dengan norma-norma sosial yang berlaku. Penggunaan teknologi internet telah membentuk masyarakat dunia baru yang tidak lagi

[1]Sambutan Prof. Dr. Barda Nawawi Arief, SH, dalam *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*. Oleh Al Wisnubroto, (Yogyakarta: Universitas Atmajaya, 1999), hal. 1.

[2]Dimitri Mahayaan, *Menjemput Masa depan, Uturistik, dan Rekayasa Masyarakat Menuju Era Global*, (Bandung: Rosda, 2000), hal. 24-25.

[3]Lihat Radian Adi Nugraha, *Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, (Depok: FH, Universitas Indonesia, 2012).

[4]Ahmad M. Ramli, *Cyberlaw dan HAKI dalam Sistem Hukum di Indonesia*, 2004, hal. 1.

dihalangi oleh batas-batas teritorial suatu negara yang dahulu ditetapkan sangat esensial sekali, yaitu dunia maya dunia yang tanpa batas, realitas virtual (*virtual reality*). Inilah yang sebenarnya dimaksud dengan *Bordelles World*.[5]

Meningkatnya pemanfaatan teknologi (seperti internet) melahirkan tantangan baru dalam perlindungan atas kepemilikan pribadi, khususnya data pribadi, terutama dalam peningkatan dalam praktik pengumpulan, pemanfaatan, dan penyebaran data pribadi seseorang. Dalam penyelenggaraan jasa telekomunikasi, perlindungan data pribadi pelanggan merupakan hal penting dalam upaya membangun hubungan hukum yang jelas antar pelaku usaha dengan pelanggan telekomunikasi. Saat ini terdapat beberapa ketentuan hukum yang terkait dengan perlindungan data pribadi yang terdiri dari yang umum (*lex generalis*) samoai dengan yang khusus (*lex specialis*), namun dapat dipahami dari peraturan yang tersedia mengenai perlindungan data pribadi di Indonesia belum terkodifikasi dalam satu peraturan sehingga belum secara komprehensif sesuai dengan prinsip-prinsip perlindungan.

Era informasi ditandai dengan aksesibilitas informasi yang sangat tinggi sebagai komoditi utama yang diperjualbelikan sehingga akan muncul berbagai *network and information company* yang akan memperjualbelikan berbagai fasilitas bermacam jaringan dan berbagai basis data informasi berbagai hal yang dapat diakses oleh pengguna dan pelanggan.[6]Bahwa internet menghadirkan *cybercpace* dengan realitas virtual banyak menawarkan kepada masyarakat dengan berbagai macam dan harapan, dimana ada sisi negatif maupun positif. Sehingga timbul permasalahan kejahatan yang disebut *Cyber Crime*, baik sistem jaringan komputernya itu sendiri yang menjadi sasaran maupun komputer itu sendiri yang menjadi sasaran kejahatan. Informasi telah menjadi komoditi utama, sehingga berbagai upaya sangat diperlukan untuk melindungi dari tindak kejahatan. *Cyber Crime* merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet sebagai perbuatan melawan hukum yang dilakukan menggunakan internet yang berbasis pada kecanggihan teknologi, komputer, dan telekomunikasi baik untuk memperoleh keuntungan ataupun tidak dengan merugikan pihak lain.

[5]Onno W. Pura dalam Agus Rahardjo, *Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Aditya Bhakti, 2014), hal. 5.

[6]Dimitri Mahayana, *Op. Cit.*, hal. 57.

Dikatakan Barda Nawawi Arif, bahwa kejahatan *Cyber Crime* dibagi menjadi 2 (dua) kategori, yaitu *Cyber Crime* dalam pengertian sempit (kejahatan terhadap sistem komputer) dan *Cyber Crime* dalam pengertian luas (mencakup kejahatan terhadap sistem komputer dan kejahatan menggunakan sarana komputer).[7] Istilah-istilah yang tetap digunakan adalah pengertian kejahatan terhadap komputer (*Crime directed at computer*), kejahatan dengan mendayagunakan komputer (*Crime utilizing computers*), kejahatan yang berkaitan dengan komputer (*Crime related to computer*), walaupun istilah-istilah tersebut belum memberikan gambaran-gambaan yang tepat. Walaupun demikian, istilah apapun yang digunakan, berbagai pihak telah berusaha mendefinisikan sendiri-sendiri berdasarkan pemahamannya.[8]

Karakteristik *Cyber Crime* dalam kejahatan konvensional, terbagi menjadi 2 (dua) jenis kejahatan, yaitu: kejahatan kerah biru (*Blue Collar Crime*) dan Kejahatan kerah putih (*White Collar Crime*). Kejahatan kerah biru merupakan kejahatan atau tindak kriminal yang dilakukan secara konvensional seperti: perampokan, pembunuhan, pencurian, dan lain-lain. Sedangkan kejahatan kerah putih terbagi menjadi kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu. *Cyber Crime* sebagai kejahatan yang muncul akibat adanya komunitas dunia maya di internet yang memiliki karakteristik unik dari kejahatan di dunia maya, antara lain: ruang lingkup kejahatan, sifat kejahatan, modus, dan jenis-jenis kerugian yang ditimbulkan.

Mengingat terus meningkatnya kasus-kasus *Cyber Crime* di Indonesia, maka pemerintah mengambil kebijakan untuk menaggulangi kejahatan tersebut. Bahwa kebijakan menentukan suatu perbuatan tindak pidana, sehubungan dengan kenyataan bahwa undang-undang memberikan wewenang dan dasar legitimasi kepada penegak hukum untuk menyatakan apakah perbuatan seseorang merupakan kejahatan atau tidak. Tetapi undang-undang dapat juga merupakan faktor kriminogen apabila tidak konsisten dengan kenyataan, terpisah dengan nilai-nilai masyarakat sehingga muncul sikap tidak percaya mengenai efektivitas sistem hukum tersebut.[9]

[7]Barda Nawawi Arif, *Tindak Pidana Mayantara dan Perkembangan kajian Cyber Crime di Indonesia,* (Jakarta: Rajawali Pers, 2006), hal. 25.

[8]*Ibid.*, hal. 211.

[9]Barda Nawawi Arif, *Penetapan Pidana Dalam Perundang-Undangan Dalam Rangka usaha Penanggulangan Kejahatan (Disertasi),* (Bandung: Universitas Padjadjaran, 1986), hal. 4-5.

B. Rumusan Masalah

Berdasarkan penulisan tentang Kebijakan Kriminal terhadap Kejahatan Dunia Maya (*Cyber Crime*) di Indonesia, maka permasalahan yang hendak dirumuskan sebagai berikut:

1. Bagaimana Kebijakan Kriminalisasi Terhadap Kejahatan Dunia Maya (*Cyber Crime*) di Indonesia?
2. Bagaimana Penanggulangan dan Penegakan Hukum terhadap Kejahatan Dunia Maya (*Cyber Crime*) di Indonesia

C. Metode Penelitian

Jenis penulisan ini menggunakan Penelitian kepustakaan (*library research*), yaitu penelitian yang mempunyai objek sumber-sumber tertulis, seperti buku-buku, jurnal, ensiklopedi dan sumber tulisan lainnya yang memiliki relevansi dengan masalah yang dibahas.[10] Metode pendekatan yang digunakan dalam penulisan ini adalah pendekatan normatif,[11] untuk mengetahui kebijakan kriminal dalam penaggulangan kejahatan dunia maya (*Cyber Crime*) di Indonesia. Teknik Pengumpulan data yang digunakan dalam penulisan ini adalah penelusuran naskah, yaitu dengan mengkaji sumber-sumber yang terkait dengan data primer (bahan-bahan yang mengikat) dan data sekunder (data yang memberikan penjelasan terhadap bahan-bahan primer, karya-karya lain yang berkaitan dengan pokok masalah yang memiliki relevansi dengan penulisan jurnal ilmiah ini. Data tertier, yaitu bahan yang memberikan petunjuk atau penjelasan data primer dan skunder dianntaranya menggunakan berbagai kamus, ensiklopedi, jurnal, dan situs-situs.[12]

D. Hasil Penelitian dan Pembahasan

1. Kebijakan Kriminalisasi Terhadap Kejahatan Dunia Maya (*Cyber Crime*) di Indonesia

Sejarah *Cyber Crime* terjadi bermula dari kegiatan *hacking* yang telah lebih dari satu abad. Pada tahun 1870-an beberapa remaja telah merusak sistem telepon baru negara dengan merubah otoritas. Pada awal tahun 1960, fasilitas universitas

[10]Kartini Kartono, *Pengantar Metodologi Riset Sosial,* (Bandung: Mandar Maju, 1996), hal. 33.

[11]Pendekatan Normatif adalah studi yang memandang masalah dari sis legal-formalnya dan/atau normatifnya. Lihat Khoirudin nasution, *Pengantar Studi Islam,* hal. 141.

[12]Soerjono Soekanto, *Pengantar Penelitian Hukum,* (Jakarta: UI-Press, 1986), hal. 52.

dengan kerangka komputer yang besar, seperti laboratorium kepintaran buatan (*artificial intelligence*) menjadi tahap percobaan bagi para *hacker* (seseorang yang menguasai komputer yang membuat sebuah program melebihi apa yang dirancang melakukan tugasnya). Di sini *Hacker* merupakan orang yang melakukan kejahatan komputer yaitu sebagai pengguna komputer secara *illegal.* Banyak jenis kejahatan *Cyber Crime,* diantaranya: *Cyber Crime* tindakan kejahatan murni, *Cyber Crime* yang menyerang individu, *Cyber Crime* yang menyerang hak cipta (hak milik), dan *Cyber Crime* yang menyerang pemerintah.

Hukum merupakan pencerminan dari suatu peradaban, kebudayaan, dan hukum juga merupakan jalinan yang erat (saling berkaitan satu dengan yang lainnya). Hukum merosot ke dalam suatu dekedansi, jika kekurangan-kekurangan dari pembentuk hukum memperlihatkan ketertinggalan berkenaan dengan fakta-fakta dan pemikiran-pemikiran yang berlaku atau mulai berkembang.[13] Ilmu kebijakan dalam hukum pidana merupakan suatu seni yang rasional, guna mencapai tujuan nasional di bidang hukum pidana dengan segala fungsi dan peranan sosialnya yang diemban melalui kebijakan hukum pidana.[14] Pranata utama yang menghasilkan kebijakan kriminal meliputi lembaga legislatif, sistem peradilan pidana, dan lembaga-lembaga pembuat kebijakan yaitu berbagai lembaga birokrasi yang diberi kewenangan untuk mengatur hal-hal yang berhubungan dengan pengendalian kejahatan dengan berbagai bentuk.

Istilah sebagai "Politik Hukum Pidana". Dalam kepustakaan dikenal dengan berbagai istilah-istilah kebijakan berasal dari kata "*Policy*" (Inggris) atau "*Politiek*" (Belanda). Bertolak dari pengertian tersebut, maka kebijakan hukum pidana dapat disebut sebagai "Politik Hukum Pidana". Dalam kepustakaan dikenal dengan berbagai istilah yakni: *"Penal Policy", "Criminal Law Policy",* atau *"Straffrechtspolitiek'.*[15]Kebijakan kriminal merupakan suatu bentuk kebijakan yang diambil oleh suatu negara untuk melakukan kriminalisasi terhadap suatu tindakan yang dianggap merugikan, serta strategi untuk meanggulanginya. Dengan merujuk pada 3 (tiga) peran utama dari kebijakan, yaitu pembuatan kebijakan, pelaksanaan

[13]Syaiful Bakhri, *Kebijakan Kriminal Dalam Perspektif Pembaruan Sistem Peradilan Pidana di Indonesia,* (Yogyakarta: Total Media, 2010), hal. 6.
[14]*Ibid.,* hal. 8.
[15]*Ibid.,* hal. 13.

kebijakan, dan advokasi kebijakan,[16]maka kebijakan kriminal dapat diartikan sebagai pembuatan, pelaksanaan, dan advokasi kebijakan yang diambil oleh negara dalam mengatasi masalah kejahatan.

Dikatakan Muladi, Kebijakan Kriminal (*Criminal Policy*) adalah sebagai usaha rasional masyarakat meanggulangi kejahatan, yang secara operasional dapat dilakukan melalui sarana penal atau non penal, dimana kedua sarana ini merupakan suatu keterkaitan yang tidak dapat dipisahkan satu sama lain, dan keduanya saling melengkapi dalam usaha penanggulangan kejahatan di masyarakat. Selanjutnya menurutnya, bahwa peanggulangan kejahatan melalui sarana penal lazimnya secara operasional dapat dilakukan melalui langkah-langkah: perumusan norma-norma hukum pidana, yang di dalamnya terkandung unsur substantif, struktural, dan kultur masyarakat, dimana sistem hukum pidana itu diberlakukan. Sistem hukum pidana yang berhasil tersebut, selanjutnya secara operasional bekerja melalui sistem, yang disebut Sistem Peradilan Pidana (*Criminal Justice System*).[17]

Kebijakan kriminal pada dasarnya terbagi menjadi 2 (dua), yaitu: *Pertama,* kebijakan pencegahan sebelum terjadinya kejahatan, dan yang *kedua* kebijakan penegakan hukum (reaktif formal) setelah terjadinya kejahatan. Ranah kebijakan kriminal yang kedua adalah menjadi kewenangan penuh Sistem Peradilan Pidana (SPP). Hanya SPP yang dapat melakukan penyelidikan, penyidikan, dan memberikan pidana terhadap pelaku kejahatan. Kebijakan kriminal lebih berfokus kepada strategi negara untuk menghindarkan masyarakat dari berbagai macam bentuk kejahatan, yaitu salah satunya menjalankan SPP. Sedangkan kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi, pada hakikatnya kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*Criminal Policy*) dengan menggunakan sarana hukum pidana (penal), dan oleh karena itu merupakan bagian dari "kebijakan hukum pidana (*penal policy*) khususnya

[16]F. James Gilsinan, *Criminology and Public Policy and Introduction*, (Englewood Clirffs: Prentice Hall, 1990), hal. 29.

[17]Muladi, *Kapita Selekta Peradilan Pidana,* (Semarang: Undip, 1995), hal. 7.

kebijakan formulasinya.[18] Disini dapat dikatakan bahwa kriminalisasi dimaksudkan proses penetapan suatu perbuatan orang sebagai perbuatan yang dapat dipidana.

Kriminalisasi muncul ketika kita dihadapkan pada suatu perbuatan yang merugikan orang lain atau masyarakat yang hukumnya belum ada atau belum ditemukan. Dengan demikian keterkaitan dengan kebijakan kriminalisasi terhadap tindak pidana *Cyber Crime*, diantaranya:

a. Persoalan kriminalisasi timbul karena di hadapan kita terdapat perbuatan yang berdimensi baru, sehingga muncul pertanyaan adakah hukumnya untuk perbuatan tersebut.[19]Sebenarnya dalam persoalan *Cyber Crime* tidak ada kekosongan hukum, hal ini terjadi digunakan metode penafsiran yang dikenal dalam ilmu hukum yang semestinya dipegang oleh aparat penegak hukum dalam menghadapi perbuatan-perbuatan berdimensi baru yang secara khusus belum diatur dalam undang-undang.[20]
b. Apabila dilihat dari pengertian kriminalisasi, sesungguhnya kriminalisasi tidak harus berupa undang-undang khusus di luar KUHP, dapat juga tetap dalam koridor KUHP melalui amandemen. Akan tetapi, proses antara membuat amandemen KUHP dengan undang-undang khusus hampir sama, baik dilihat dari berbagai segi, waktu maupun biaya, dan ketidaktegasan sistem hukum kita yang tidak menganunt sistem kodifikasi mutlak yang menyebabkan munculnya bermacam-macam undang-undang khusus.
c. Dalam hal ini kriminalisasi berkaitan dengan masalah harmonisasi, yaitu harmonisasi substansi (materi) dan harmonisasi eksternal (internasional atau global). Berkaitan dengan harmonisasi substansi tidak banyak KUHP yang berdampak dari dibuatnya undang-undang *Cyber Crime.*

[18]Barda Nawai Arif, *Pembaharuan Hukum Pidana Dalam perspektif Kajian Perbandingan,* bandung: Citra Aditya Bhakti, 2005, hlm. 126. Lihat juga dalam barda nawawi Arif, *Tindak Pidana Mayantara, Perkembangan Cyber Crime di Indonesia,* Jakarta: Raja Grafindo Persada, 2006, hal. 90. Lihat juga pengertian Kriminalisasi dari Sudarto, *Hukum dan Hukum Pidana,* (Bandung: Alumni, 1896), hal. 32 dan 151.

[19]Rony Nitibaskara, *Problem Yuridis Cyber Crime,* Makalah pada Seminar tentang *Cyber Law* diselenggarakan oleh yayasan Cipta Bangsa, (Bandung: tanggal 29 Juli 2000), hal. 2 dan 5.

[20]Upaya penafsiran *Cyber Crime* ke dalam perundang-undangan khususnya Kitab Undang-Undang Hukum Pidana telah dilakukan baik oleh instansi maupun individual. Lihat Badan Pembinaan Hukum Nasional, Perkembangan Pembangunan Hukum Nasional tentang Hukum Teknologi dan Informasi, BPHN: Departemen kehakiman Republik Indonesia, 1995/1996, hal. 32-34.

Bahwa Kementrian Komunikasi dan Informasi Republik Indonesia mencatat ada 21 undang-undang dan 25 (dua lima) Rancangan Undang-Undang yang akan terkena dampak dengan dikeluarkan undang-undang *Cyber Crime.* Persoalan harmonisasi eksternal berupa penyesuaian perumusan pasal-pasal *Cyber Crime*dengan ketentuan yang serupa dengan negara lain. Hal ini menunjukkan bahwa persoalan harmonisasi merupakan persoalan yang terus menerus dengan diundangkannya undang-undang yang mengatur *Cyber Crime.* Judge Schjolberg dan Amanda H. Hubbar, mengatakan bahwa persoalan *Cyber Crime*diperlukan standarisasi dan harmonisasi dalam 3 (tiga) era, yaitu *legislation, criminal enforcement, d*an *judicial review.*[21]

d. Bahwa *Cyber Crime*merupakan kejahatan yang menggunakan teknologi komputer, sehingga diperlukan modifikasi jenis sanksi pidana terhadap pelaku tindak pidana tersebut. Pertanggungjawaban *Internet Service Provider* (ISP) sebagai penyedia layanan internet apakah bersifat individu atau korporasi sebagai bentuk pertanggungjawaban, bagi pelaku yang terlibat *Cyber Crime.*

Dikatakan Al Wisnubroto, bahwa upaya kriminalisasi terhadap tindak pidana mayantara (*Cyber Crime*) harus mempertimbangkan 3 (tiga) hal, sebagai berikut:[22]

a. Hendaknya dipilih perbuatan yang benar-benar merugikan dan dapat menimbulkan akses serius (prinsip selektif dan limitatif), agar pengaturan perbuatan yang dikategorikan sebagai tindak pidana mayantara tidak bersifat *over criminalization* sehingga akan berdampak *counter productive* bagi pengembangan teknologi komputer di bidang multimedia atau teknologi informasi yang sangat dibutuhkan oleh negara Indonesia dalam menghadapi era globalisasi.

[21]Judge Stenin Schjolberg dan Amanda M. Hubbard, *Harmonizing National legal Approaches on Cyber Crime, WSISThematic Meeting on Cyber Security*, ITU, Genewa, 28 Juni-11 July 2005, Document: CYB/04, 10 June 2005, dapat dijumpai di http:// www.itu.int/ osg/ cybersecurity/ doc/ Background_ Paper_Harmonizing_National_ and_Legal_Approaches_on_Cybercrime.pdf, diakses tanggal 5 November 2018.

[22]Al Wisnubroto, *Cyber Crime, Permasalahan dan Penanggulangan dari Aspek Hukum Pidana, Diskusi Bagian Kepidanaan*, (Yogyakarta: Universitas Muhammadiyah Yogyakarta, 2000), hal 12.

b. Hendaknya mempertimbangkan apakah biaya yang harus dikeluarkan untuk menyusun ketentuan yang mengatur delik komputer sebagai tindak pidana mayantara bersifat rumit dan kompleks, sehingga biaya untuk mengawasi dan menegakkan ketentuan tersebut yang memerlukan fasilitas dan sarana teknologi yang tinggi beban yang harus dipikul korban akan berimbang dengan hasil, yaitu situasi tertib hukum dari dunia mayantara (*cost and benefit principle*),
c. Hendaknya dipertimbangkan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum di Indonesia, yang nantinya akan dibebani tugas untuk menegakkan ketentuan yang mengatur delik komputer yang dikategorikan sebagai tindak pidana mayantara, sehingga tidak terjadi beban tugas yang bersifat *overbelasint* sehingga banyak peraturan yang dibuat ternyata dalam praktiknya di lapangan tidak dapat ditegakkan.

Suatu pengaturan yang secara khusus diperlukan apabila tindak pidana mayantara (*Cyber Crime*) dianggap sebagai kejahatan kategori baru (*new category of crime*) yang membutuhkan suatu kerangka hukum baru dan komprehensif untuk mengatasi sifat khusus teknologi yang sedang berkembang dan tantangan baru yang tidak ada pada kejahatan biasa, karena itu perlu diatur secara tersendiri di luar KUHP.[23]Dikatakan Muladi, bahwa dalam mempidana atau mengkriminalisasikan harus memperhatikan syarat-syarat yang sifatnya limitatif karena hukum pidana bersifat *ultimum remidiuim,* diantaranya:[24]

a. Jangan menggunakan hukum pidana untuk membalas dengam semata-mata;
b. Jangan menggunakan hukum pidana, jika korbannya tidak jelas;
c. Jangan menggunakan hukum pidana jika ada cara-cara lain yang lebih efektif;

[23]Mardjono Reksodiputro, *Cyber Crime: Intelectual Property Rights-E Commerce,* Penataran Nasional Hukum Pidana dan Kriminologi Indonesia (ASPEHUPIKI), di Fakultas Hukum Surabaya, pada tanggal 13-19 Januari 2002.

[24]Muladi, dalam makalah seminar *"Kejahatan Terhadap Kepentingan Umum dan kejahatan terhadap Martabat Dilihat dari Sudut Pandang Hak Asasi Mannusia,* Komisi nasional Hak Asasi Manusia Lembaga Studi dan Advokasi Masyarakat (ELSAM), Fakultas Hukum Universitas Udayana, pada tanggal 20-21 Maret 2006.

d. Jangan menggunakan hukum pidana jika kerugian pembiayaan akibat dari pemidanaan lebih besar daripada kerugian pembiayaan akibat tindak pidana sendiri;
e. Jangan menggunakan hukum pidana jika efek sampingnya lebih besar dari perbuatan yang dikriminalisasikan;
f. Jangan menggunakan hukum pidana jika tidak mendapat dukungan dari masyarakat luas;
g. Jangan menggunakan hukum pidana apabila hukum tersebut diperkirakan tidak bisa berlaku secara efektif;
h. Hukum pidana harus bisa menjaga kepentingan negara, individu, serta masyarakat; dan
i. Harus selaras dengan sifatnya yang non-penal.

2. Penanggulangan dan Penegakan Hukum Terhadap Kejahatan Dunia Maya (*Cyber Crime*) di Indonesia.

Untuk menaggulangi kejahatan internet yang semakin meluas,diperlukan suatu kesadaran akan bahaya penggunaaan internet, diantaranya:

a. Adanya modernisasi hukum pidana beserta hukum acaranya diselaraskan terkait kejahatan dunia maya (*Cyber Crime*);
b. Peningkatan standar pengamanan system jaringan komputer;
c. Meningkatkan pemahaman serta keahlian aparat hukum; dan
d. Meningkatkan kesadaran akan bahaya *Cyber Crime*dan mencegah kejahatan terebut.

Penegakan hukum *Cyber Crime*di Idonesia sangat dipengaruhi oleh 5 (lima) faktor, yaitu undang-undang, mentalitas aparat penegak hukum, perilaku masyarakat, sarana dan kultur. Hukum tidak bisa tegak dengan sendirinya karena selalu melibatkan manusia dan tingkah laku manusia di dalamnya. Selain itu, hukum juga tidak bisa tegak tanpa adanya aparat penegak hukum. Oleh sebab itu, aparat penegak hukum dituntut profesional dalam menerapkan norma hukum dalam menghadapi pelaku tindak kejahatan. Kitab Undang-Undang Hukum Pidana menjadi dasar untuk menjaring *Cyber Crime,* yang memenuhi unsur-unsur dalam pasal-pasal KUHP.

Selain KUHP ada juga aturan hukum yang berkaitan dengan hal ini, yaitu Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), dimana aturan tindak pidana yang terjadi di dalamnya terbukti mengancam para pengguna internet. Pasal-pasal dalam UU ITE Tahun 2008 sebagai payung hukum bagi masyarakat pengguna teknologi guna mencapai kepastian hukum tidak mengalami perubahan dalam UU ITE Tahun 2016 (Revisi baru), sebagai berikut:

a. Pasal 27 UU ITE Tahun 2008, berbunyi: *"Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan melanggar kesusilaan".* Ancaman pidana terdapat pada Pasal 45 Ayat (1) KUHP dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,- (satu miliar rupiah).
b. Pasal 28 UU ITE Tahun 2008, berbunyi: *"Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik".*
c. Pasal 29 UU ITE Tahun 2008, berbunyi: *"Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditunjukkan secara pribadi (Cyber Stalking)".* Ancaman pidananya terdapat pada Pasal 45 Ayat (3) KUHP, setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 2.000.000.000,- (dua miliar).
d. Pasal 30 UU ITE Tahun 2008 Ayat (3): *"Setiap orang yang dengan sengaja tanpa hak atau melawan hukum mengakses computer dan/atau system elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengaman (cracking, hacking, illegal acces).* Ancaman pidana terdapat pada Pasal 46 Ayat (3): *"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 Ayat (3) dipidana penjara dengan pidana penjara paling lama 8 (delapan)*

dan/atau denda paling banyak Rp. 800.000.000,- delapan ratus juta rupiah)".

e. Pasal 33 UU ITE Tahun 2008: *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya system elektronik dan/atau mengakibatkan system elektronik menjadi tidak bekerja sebagaimana mestinya".*

f. Pasal 34 UU ITE Tahun 2008: *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki".*

g. Pasal 35 UU ITE Tahun 2008: *"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut seolah-olah data yang otentik (Phising=penipuan situs)".*

Kitab Undang-Undang Hukum Pidana, Pasal 362 KUHP yang dikenakan untuk kasus carding, Pasal 378 KUHP dapat dikenakan untuk penipuan, dan Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkannya. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.

Berdasarkan Pasal 1 Angka (9) Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, berbunyi: *"Program komputer adalah seperangkat instruksi yang diekspresikan dalam bentuk bahasa , kode, skema, atau dalam bentuk apapun yang ditujukan agar komputer bekerja melakukan fungsi tertentu atau untuk mencapai hasil tertentu".*

Berdasarkan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi pasal 1 Angka (1) berbunyi: *"Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk*

tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya".

Berdasarkan Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan. *"Pemerintah berusaha untuk mengatur pengakuan atas mikrofil dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau atau ditransformasikan".*

E. Penutup

1. Simpulan

Dari uraian-uraian tersbut di atas, Penulis menarik kesimpulan dari penulisan ini sebagai berikut:

a. Kebijakan kriminal (*Criminal Policy*) adalah sebagai usaha rasional masyarakat menanggulangi kejahatan, yang secara operasional dapat dilakukan baik melalui sarana penal maupun non-penal, dimana kedua sarana ini merupakan suatu keterkaitan yang tidak dapat dipisahkan satu sama lain, dan keduanya saling melengkapi dalam usaha penaggulangan kejahatan di masyarakat. Penanggulangan kejahatan melalui sarana penal lazimnya secara operasional dapat dilakukan melalui langkah-langkah: perumusan norma hukum pidana, yang di dalamnya terkandung unsur substantif, struktural, dan kultur masyarakat, dimana sistem hukum pidana itu diberlakukan. Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan dipidana)). Jadi, pada hakikatnya kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*Criminal Policy*) dengan menggunakan sarana hukum pidana (penal), dan oleh sebab itu merupakan bagian dari "Kebijakan Hukum Pidana (*penal policy*) khususnya kebijakan formulasinya.

b. Penegakan hukum *Cyber Crime* di Indonesia sangat dipengaruhi oleh 5 (lima) faktor, yaitu undang-undang, mentalitas aparat penegak hukum, perilaku masyarakat, sarana dan kultur. Hukum tidak bisa tegak dengan sendirinya karena selalu melibatkan manusia dan tingkah laku manusia di dalamnya. Selain itu, aparat penegak hukum juga tidak bisa tegak tanpa adanya aparat penegak hukum.

Karenanya, aparat penegak hukum dituntut prifesional dalam menerapkan norma hukum dalam menghadapi pelaku tindak kejahatan. Kitab Undang-Undang Hukum Pidana menjadi dasar untuk menjaring *Cyber Crime*, yang memenuhi unsur-unsur dalam pasal-pasal Kitab Undang-Undang Hukum Pidana (KUHP). Selain KUHP ada juga aturan hukum yang berkaitan dengan hal ini, yaitu Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), dimana aturan tindak pidana yang terjadi di dalamnya terbukti mengancam para pengguna internet.

2. Saran

a. Sebaiknya pemerintah dalam hal ini aparat penegak hukum dalam menangani *Cyber Crime*melakukan *self protection* terhadap data atau informasi yang terdapat dalam jaringan komputer yang merupakan ujung tombak dari pencegahan dan penanggulangan *Cyber Crime.*

b. Sebaiknya, masyarakat luas dalam menggunakan teknologi informasi, dalam hal internet adalah untuk sarana yang positif, yaitu sebagai bahan informasi pengetahuan, sehingga menambah wawasan keilmuan dalam bermasyarakat, berbangsa, dan bernegara.

Daftar Pustaka

Buku

Ahmad M. Ramli, *Cyberlaw dan HAKI dalam Sistem Hukum di Indonesia,* 2004.

Adian Adi Nugraha, *Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik,* (Depok: FH, Universitas Indonesia, 2012).

Al Wisnubroto, *Cyber Crime, Permasalahan dan Penanggulangan dari Aspek Hukum Pidana, Diskusi Bagian Kepidanaan,* (Yogyakarta: Universitas Muhammadiyah Yogyakarta, 2000).

Barda Nawawi Arif, *Tindak Pidana Mayantara dan Perkembangan kajian Cyber Crime di Indonesia,* (Jakarta: Rajawali Pers, 2006).

……., *Penetapan Pidana Dalam Perundang-Undangan Dalam Rangka usaha Penanggulangan Kejahatan (Disertasi),* (Bandung: Universitas Padjadjaran, 1986).

……..... *Pembaharuan Hukum Pidana Dalam perspektif Kajian Perbandingan,* bandung: Citra Aditya Bhakti, 2005. 126. Lihat juga dalam barda nawawi Arif, *Tindak Pidana Mayantara, Perkembangan Cyber Crime di Indonesia,* Jakarta: Raja Grafindo Persada, 2006, hlm. 90. Lihat juga pengertian Kriminalisasi dari Sudarto, *Hukum dan Hukum Pidana,* (Bandung: Alumni, 1896).

……., dalam *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer.* Oleh Al Wisnubroto, (Yogyakarta: Universitas Atmajaya, 1999).

……., *Kapita Selekta Hukum Pidana,* (Bandung: Citra Aditya Bhakti, 2003).

Dimitri Mahayaan, *Menjemput Masa depan, Uturistik, dan Rekayasa Masyarakat Menuju Era Global*, (Bandung: Rosda, 2000).

Kartini Kartono, *Pengantar Metodologi Riset Sosial,* (Bandung: Mandar Maju, 1996).

James Gilsinan, *Criminology and Public Policy and Introduction,* Englewood Clirffs: Prentice Hall, 1990.

Muladi, *Kapita Selekta Peradilan Pidana,* (Semarang: Undip, 1995).

Onno W. Pura dalam Agus Rahardjo, *Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Aditya Bhakti, 2014).

Radian Adi Nugraha, *Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik*, (Depok: FH, Universitas Indonesia, 2012).

Soerjono Soekanto, *Pengantar Penelitian Hukum*, (Jakarta: UI-Press, 1986).

Syaiful Bakhri, *Kebijakan Kriminal Dalam Perspektif Pembaruan Sistem Peradilan Pidana di Indonesia*, (Yogyakarta: Total Media, 2010).

Pidato/Penataran/Makalah

Mardjono Reksodiputro, *Cyber Crime: Intelectual Property Rights-E Commerce*, Penataran Nasional Hukum Pidana dan Kriminologi Indonesia (ASPEHUPIKI), di Fakultas Hukum Surabaya, pada tanggal 13-19 Januari 2002.

Muladi, dalam makalah seminar *"Kejahatan Terhadap Kepentingan Umum dan kejahatan terhadap Martabat Dilihat dari Sudut Pandang Hak Asasi Mannusia*, Komisi nasional Hak Asasi Manusia Lembaga Studi dan Advokasi Masyarakat (ELSAM), Fakultas Hukum Universitas Udayana, pada tanggal.

Rony Nitibaskara, *Problem Yuridis Cyber Crime*, Makalah pada Seminar tentang *Cyber Law* diselenggarakan oleh yayasan Cipta Bangsa, (Bandung: tanggal 29 Juli 2000).

Website

Judge Stenin Schjolberg dan Amanda M. Hubbard, *Harmonizing National legal Approaches on Cyber Crime, WSISThematic Meeting on Cyber Security*, ITU, Genewa, 28 Juni-11 July 2005, Document: CYB/04, 10 June 2005, dapat dijumpai di http:// www.itu.int/ osg/ cybersecurity/ doc/ Background_ Paper_ Harmonizing_National_ and_Legal_ Approaches_on_ Cybercrime.pdf, diakses tanggal 5 November 2018.